

# 2020 Q2 Hyperledger Ursa

## Project

This is the report of the Ursa project.

## Project Health

Ursa has been in a relatively stable state recently, which is nice considering the Sovrin foundation let go of all of its technical staff, some of whom contributed extensively to Ursa (and thankfully still are). We are continuing work on "fancy" crypto primitives like zero knowledge proofs. We have substantially improved the efficiency of some of our elliptic-curve based primitives recently, which should hopefully make adoption more compelling.

## Questions/Issues for the TSC

We are always interested in getting in touch with others who want to use cryptography, and particularly so for people that want to use non-standardized crypto like threshold signatures or zero knowledge proofs. If this describes you, please feel free to get in touch with us.

## Releases

We've had two releases since the last report, which focused on BBS+ signatures.

April 29: bbs-v0.3.0

May 18: bbs-v0.4.0

## Overall Activity in the Past Quarter

- Added and improved BBS+ signatures
- Switched our core pairings library from Milagro to pairing-plus (Apache 2.0 licensed). This gives us both much better efficiency and probably more security, since pairing-plus seems to be better maintained than the Apache-licensed version of Milagro.
- Implemented efficient "hash to curve" functionality.

## Current Plans

- Add WASM support for BBS+ signatures.
- Continue with our work on trusted hardware.

## Maintainer Diversity

### Current Active Maintainers:

- Mike Lodder (Sovrin Foundation)
- Brent Zundel (Evernym Inc.)
- Dave Huseby (Linux Foundation)
- Hart Montgomery (Fujitsu)
- Dan Middleton (Intel)
- Cam Parra (Kiva)
- Dan Anderson (Intel)
- Jon Geater (Jitsuin)

## Contributor Diversity

### Current Contributor Affiliations:

- Evernym, Inc
- Intel
- BCGov
- Iqlusion
- Jitsuin
- Fujitsu

We would especially like to note that our most prolific contributor (Mike Lodder) is now an independent contributor (so if you are hiring, take note). In addition, we would like to thank the BCGov team for contributing quite a bit this quarter.

## Additional Information

Ursa meeting attendance has increased a bit as of late, although this has not directly translated (hopefully yet) into more contributors.

## Reviewed by

- Angelo De Caro
- Arnaud J Le Hors
- Christopher Ferris
- Dan Middleton
- Gari Singh
- Hart Montgomery
- Mark Wagner
- Nathan George
- Swetha Repakula
- Tracy Kuhrt
- Troy Ronda